White Paper

HardenStance

Aligning Spectrum Policy with Cybersecurity Goals

By Patrick Donegan, Principal Analyst, HardenStance

Sponsored by

ctia

May 2023

HardenStance

"Trusted Research, Analysis and Insight in IT & Telecom Security"

Executive Summary

- Spectrum policy should attach more weight to a user's incentive and ability to defend America's wireless networks against high impact cyber-attacks – whether they be by nation state adversaries like China or other cyber threat actors.
- The licensed spectrum model drives high standards, accountability, and a high degree of commonality and predictability in the way wireless carriers protect and curate spectrum assets against cyber threats. They have mature operating models for protecting the network as well as for reporting cyber incidents.
- Exclusive spectrum licensing is best for ensuring that the cybersecurity posture of users aligns with national cybersecurity and broader national security goals.

Balancing spectrum policy for a new American era

As the Federal Communications Commission (FCC) and the National Telecommunications and Information Administration (NTIA) deliberate over the release of spectrum in the lower mid-band, competing stakeholders who disagree on many details can nevertheless find themselves agreeing on the need for a "balanced" national spectrum policy.

The balance that needs to be struck is across the interests of key stakeholders such as the federal government (civilian and military); business interests with a stake in licensed spectrum (e.g. the wireless and aviation sectors) as well as the many commercial and non-commercial users of unlicensed spectrum. At a more granular level, balance is needed to ensure spectrum policy can support several different, even conflicting, macro-policy goals like business innovation, GDP growth, public safety, social inclusivity, international competitiveness, carbon footprint reduction, defence and national security.

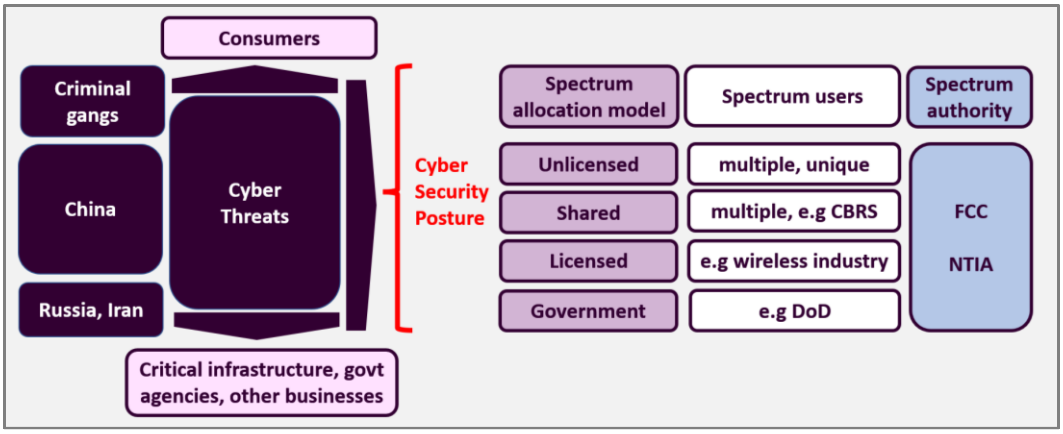
One factor that has assumed a lot more importance for upcoming spectrum policy decisions is the sharp change in America's relationship with China.

Cybersecurity should be a key factor in spectrum policy

One factor that has assumed a lot more importance for upcoming spectrum policy decisions is the sharp change in America's relationship with China. Once centred on partnership, co-dependence and collaboration, the axis of the relationship has shifted to one that is undergoing strategic de-coupling and becoming more adversarial. This has two critical implications for U.S. spectrum policy:

- There is a higher cost to sub-optimal use of spectrum because it fails to maximize the wireless innovation that is key to the U.S. economy outperforming China's.
- The increasingly adversarial nature of the relationship has triggered a sharp uptick in the severity of cyber-attacks against the U.S and its allies, most notably by Chinese and Russian threat actors. This poses a heightened national security risk to the confidentiality, integrity and availability of communications used by critical sectors of U.S industry, by other businesses, and indeed by all Americans.

Figure 1: Cybersecurity is an Increasingly Important Factor in Spectrum Policy



Source: HardenStance

Cybersecurity imperatives for a new era

This White Paper argues that aligning spectrum policy with the cybersecurity imperatives of the next ten years requires that the FCC should prioritise releasing mid-band spectrum as licensed spectrum. In particular it requires that the FCC should ensure America's wireless operators such as AT&T, Verizon and T-Mobile have the spectrum they need to enable businesses to capture the innovation and growth potential of 5G and 6G.

The paper makes this case by demonstrating that the cybersecurity ecosystem that supports licensed wireless operators is already best in class. Moreover, the way the market in wireless services is set to evolve will also create two new cybersecurity challenges that licensed wireless operators are uniquely well placed to respond to:

Aligning spectrum policy with the cybersecurity requirements of the next ten years requires that the FCC should prioritise releasing mid band spectrum as licensed spectrum.

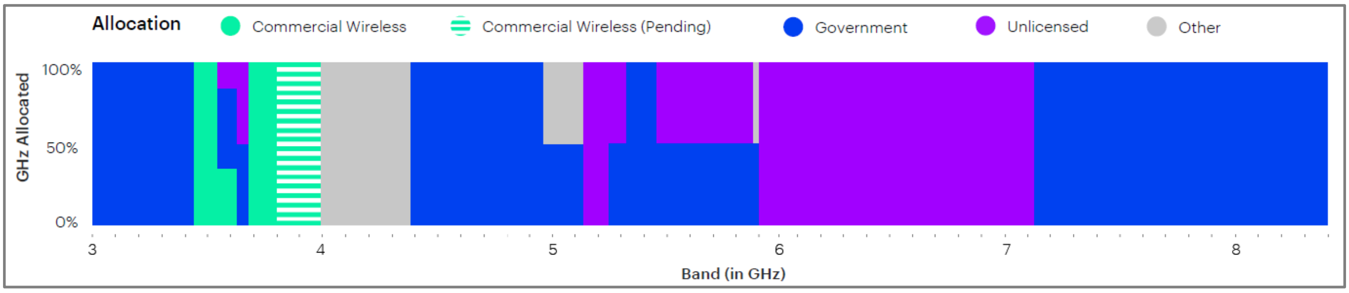
- **The first of these is the further scaling up in the volume and diversity of connected wireless devices, applications and traffic.** This is a key factor driving demand for more spectrum in the first place. But as well as all the upside in terms of growth and innovation, this inevitable trend also has a downside in the form of the extra complexity it creates in telco network operations. The dynamic scaling up of interactions between so many new and different hardware and software components at such scale will inevitably generate new vulnerabilities in telecom networks, hence new hacking opportunities.
- **The second challenge is the evolving landscape in cyber threats targeting American businesses, critical infrastructure and consumers.** Given the evidence of more audacious attacks carried out by China and other nation state hackers of late (see **Figure 3**), it's reasonable to assume that defending against cyber-attacks could become increasingly challenging, generating risk to the economy and society on an even greater scale than what we have seen in the last couple of years. There may be an even higher social and economic price to pay for failing to defend the nation's critical infrastructure against future cyber-attacks – including its telecom networks.

Cybersecurity is a critical part of national security

The critical question that has to be addressed is therefore what type of cybersecurity ecosystem is going to protect against these increased risks, which players in the ecosystem are going to lead it, and how? Policy makers need to be confident that spectrum allocation decisions are aligned with ensuring users are properly protected against cyber threats, including from a national security perspective.

The rest of this paper describes those cyber threats and why licensed operators are best placed to protect against them. As policy makers seek a 'balanced' approach in the lower mid-band, it's worth noting just how unbalanced the current state of spectrum allocation is. According to Accenture, the commercial wireless industry currently has access to only 270 MHz or around 5% of lower mid-band spectrum (See **Figure 2**). By contrast, at around 36%, unlicensed spectrum users have access to more than seven times that amount. Government has access to even more spectrum than unlicensed users. Balance surely requires rebalancing here.

Figure 2: 3 – 8.5GHz Spectrum Allocations in The United States by Use



Source: Accenture, "Spectrum Allocation in The United States", 2022

Increasingly audacious attacks on U.S interests

One of the defining trends in cybersecurity over the last three years has been the willingness of advanced cyber threat actors to pull off increasingly audacious attacks that impose an increasingly heavy price on their targets, often taking increased risk of escalating hostilities between rival or hostile nation states.

Figure 3 cites the three most high profile cyber-attacks to impact U.S interests in the last three years. The first two were on SolarWinds (discovered in December 2020) and Microsoft 'Hafnium' (discovered in March 2021), each of which exposed the confidential data of several thousand corporations and large businesses. The third was on 'Colonial Pipeline' which halted 5,500 miles of pipeline operations on the east coast in May 2021, causing major disruption to business and millions of people. All three were carried out during the two-year period before the subsequent further deterioration in relations between the U.S and both China and Russia that was triggered by the two's new "partnership with no limits" and then by Russia's invasion of Ukraine.

The SolarWinds and Hafnium breaches were attributed to Russian and Chinese nation state threat actors, respectively. Although the Colonial Pipeline hack was attributed to a Russian ransomware gang rather than the Russian state, the impact was nevertheless big enough to merit a "whole of government response" at federal level.

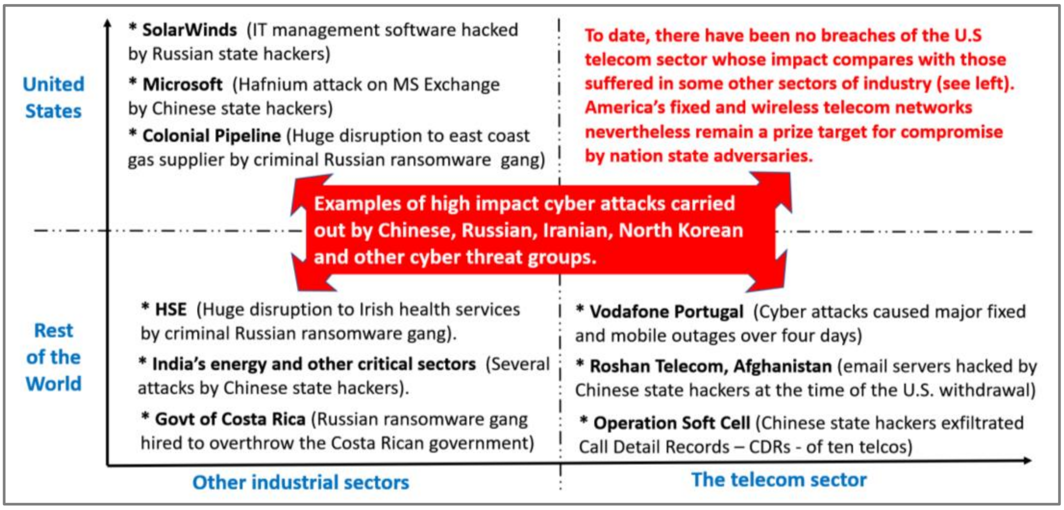
With Hafnium, Chinese state threat actors deviated from established cyber espionage norms by also booby-trapping some of the victims' infrastructure.

Some nation state threat actors are taking more and more risk

While there have been no known breaches of the U.S telecom sector whose impact compares with them, these three prominent attacks show the escalating scale of the impact – or 'blast radius' – that cyber-attacks can have on the American economy and society. They also indicate a willingness on the part of some nation state threat actors to take more and more risk and inflict more and more damage on their targets.

In the case of SolarWinds, Russian state threat actors complied with established cyber espionage norms in so far as they accessed then-unprecedented amounts of data and left it at that. With Hafnium, Chinese state threat actors deviated from these norms by also booby-trapping some victims' infrastructure. Leaving an adversary's infrastructure vulnerable to being subsequently damaged or depleted in this way increased the risk of further escalation in offensive cyber operations between the U.S and China.

Figure 3: Real World Cyber-attacks on Telecom and Other Critical Sectors



* **SolarWinds** (IT management software hacked by Russian state hackers)

* **Microsoft** (Hafnium attack on MS Exchange by Chinese state hackers)

* **Colonial Pipeline** (Huge disruption to east coast gas supplier by criminal Russian ransomware gang)

To date, there have been no breaches of the U.S telecom sector whose impact compares with those suffered in some other sectors of industry (see left). America's fixed and wireless telecom networks nevertheless remain a prize target for compromise by nation state adversaries.

Examples of high impact cyber attacks carried out by Chinese, Russian, Iranian, North Korean and other cyber threat groups.

* **HSE** (Huge disruption to Irish health services by criminal Russian ransomware gang).

* **India's energy and other critical sectors** (Several attacks by Chinese state hackers).

* **Govt of Costa Rica** (Russian ransomware gang hired to overthrow the Costa Rican government)

* **Vodafone Portugal** (Cyber attacks caused major fixed and mobile outages over four days)

* **Roshan Telecom, Afghanistan** (email servers hacked by Chinese state hackers at the time of the U.S. withdrawal)

* **Operation Soft Cell** (Chinese state hackers exfiltrated Call Detail Records – CDRs - of ten telcos)

Source: HardenStance

Telecom networks are a prize target for cyber-attacks

America’s communications networks are a prime target for cyber-attacks seeking to compromise the confidentiality, integrity and availability of the services they support. **Figure 5** is representative of the daily battles wireless operators fight to maintain the availability of their networks in the face of growing volumes of Distributed Denial of Service (DDoS) attacks. In 2023, the idea that major cyber threat actors have no current interest in breaching America’s telecom networks with greater consequences than we’ve seen to date – or that they will have no such interest in the future – simply isn’t credible.

The ban on Huawei is the most obvious example of U.S policy makers recognizing that its telecom networks are a prime target for cyber threats. But as shown below, nation state and other threat actors use many other means besides dropping malware in a domestic telecom vendor’s software to breach telecom networks around the world.

- In November 2017, the then Head of the UK’s National Cyber Security Centre (NCSC) confirmed that Russian interference in the UK that year “included attacks on the UK media, telecom and energy sector”
- In July 2019, cybersecurity vendor Cybereason published research on ‘Operation Soft Cell’ whereby Chinese state threat actors managed to exfiltrate Call Detail Records (CDRs) from a number of telecom operators using vulnerabilities in a public facing web server as the strike point for initial entry.
- In 2020, ‘Lebanese Cedar’, a cyber threat group linked to Hezbollah and Iran exploited unpatched Oracle and Atlassian servers to exfiltrate private documents from a number of operators in the Middle East and North Africa. These included Vodafone Egypt, Mobily and Etisalat.
- In September 2021, Chinese state threat actors exfiltrated 4 Gbytes of data from the email servers of Roshan Telecom in Afghanistan. The exfiltration activity spiked at the time of the U.S. troop withdrawal from the country.
- In February 2022, the fixed and mobile networks of Vodafone Portugal were severely disrupted over four days, arising from a cyber-attack which has yet to be publicly attributed to any specific threat group. Vodafone Portugal’s Chief Executive, Mário Vaz, deplored the attackers for “[shutting down] schools, hospitals, firefighters, companies, families… the lives of millions of Portuguese”.

Nation state and other threat actors use many other means besides dropping malware in a domestic telecom vendor’s software to successfully breach telecom networks.

Wireless technology risk increases markedly as IoT scales up

Better device-level security is key to protecting against the risk from billions of wirelessly-connected IoT ‘things’. But network layer security is just as critical. Licensed wireless operators can first secure, and then constantly monitor and manage every single 4G or 5G-connected IoT device in the field. With unlicensed technologies, users can connect insecure as well as insecure devices to their home or enterprise network. Some unlicensed spectrum users monitor and manage their devices but most don’t.

The risk is heightened by the increasingly critical role that wireless technologies are taking on. For example, some of the advanced industrial use cases being contemplated with 5G, 6G, Wi-Fi 6 and Wi-Fi 7 entail far more business and societal risk than anything we’ve seen before. It’s no longer just your smartphone, your PC or your wirelessly connected doorbell that are at risk – it can be industrial machinery or critical infrastructure. In the examples of attacks on telecom networks cited above, the motive in the first four cases was exposing sensitive information (a breach of confidentiality). In the fifth, it was denying services to millions of users (a breach of availability). As wireless technologies are deployed in advanced industrial use cases, including at remote sites with less robust physical protections, all these risks are in play – albeit the consequences of a breach are potentially much greater. Much closer attention also needs paying to the risk of breaches of integrity, whereby industrial processes can be interfered with by exploiting software vulnerabilities or introducing malware.

How licensed wireless operators do cybersecurity

As depicted in the NIST cybersecurity framework in **Figure 4**, the strength of any network's cybersecurity posture is determined by how well people, technology and processes are coordinated. In line with the first of the five pillars depicted that first means identifying risks and protecting against them. It also requires excellence in detecting and responding when breaches arise. Finally, cybersecurity posture is determined by how well an organization can recover from a breach. Ultimately, the security of any network – fixed or wireless, licensed or unlicensed – is only as good as its weakest link. How wireless operators using licensed spectrum practise cybersecurity is explained below in five sections: commercial incentive; security architecture; security operations; collaboration with government and wireless industry peers; and consistency.

It's true that with some aspects of a wireless user's experience it makes no difference to their cybersecurity whether they're using licensed or unlicensed spectrum. For example, Android and iOS deal with malware in exactly the same way, independently of whether it gets onto a device via 5G or Wi-Fi. In an enterprise network, a firewall provides uniform protection against unwanted traffic, independent of access network.

Ultimately, the security of any network – fixed or wireless, licensed or unlicensed – is only as good as its weakest link.

The power of a commercial incentive

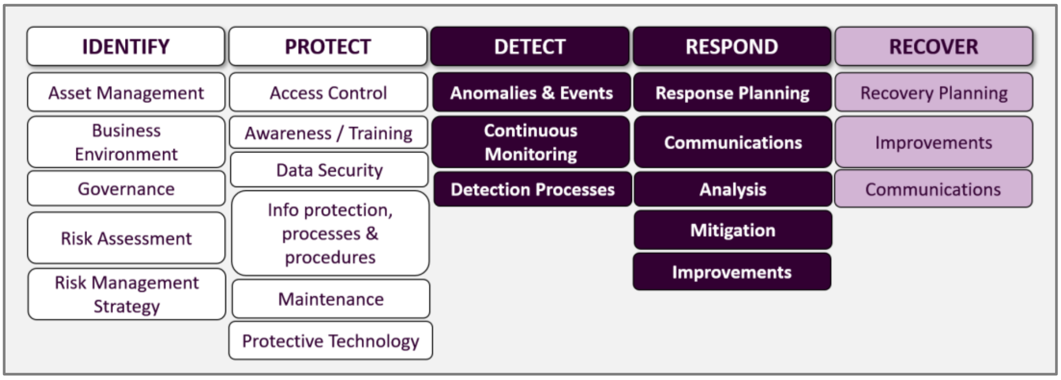
In many other ways, however, the cybersecurity ecosystem curated by licensed wireless operators is unrecognizable from the world of unlicensed spectrum. In the first place the licensed spectrum model is founded on large commercial incentives. In the 30 years since the FCC was first granted its spectrum auction authority, it has raised over $230 billion. In 'Auction 107', which made available 5G spectrum in the 3.7 GHz to 3.98 GHz band, the FCC announced in January 2021 that wireless operators had bid $81 billion.

Investment on this scale, and the need to generate a return on it, creates a huge incentive for licensed operators to protect the confidentiality, availability and integrity of their networks on behalf of all their customers who pay for using them. This commercial incentive features front and centre in a wireless operator's cybersecurity framework, including the foundational 'Identify' pillar shown in **Figure 4.**

A trillion dollar, standards-driven ecosystem

Licensed wireless operators derive the fundamentals of their network security architecture from 3GPP, the global standards body responsible for 2G, 3G, 4G and now 5G standards. Roughly speaking, 3GPP's security features map to the second 'Protect' pillar in **Figure 4.** More than 750 operators throughout the world leverage 3GPP's security standards to generate more than a trillion dollars in annual revenues according to data from the GSMA.

Figure 4: The NIST Cybersecurity Framework



IDENTIFY	PROTECT	DETECT	RESPOND	RECOVER
Asset Management	Access Control	Anomalies & Events	Response Planning	Recovery Planning
Business Environment	Awareness / Training	Continuous Monitoring	Communications	Improvements
Governance	Data Security	Detection Processes	Analysis	Communications
Risk Assessment	Info protection, processes & procedures		Mitigation	
Risk Management Strategy	Maintenance		Improvements	
	Protective Technology			

Source: HardenStance/NIST

Foundational security features of the 5G platform

Some of the foundational security features of the 5G platform are clearly differentiated:

- Like all 3GPP technologies, 5G is connection-oriented rather than connectionless. This means that in hand-off scenarios between 5G cell sites, data is only ever transferred once an encrypted connection is established between the two cell sites. That protects against the data being dropped, intercepted or re-routed.
- In 5G every user session is automatically encrypted - at home, at work and anywhere in public whilst on the move. 5G users don't have to think or worry about installing a VPN and making sure it's switched on and up to date. 5G operators don't have to worry about large numbers of their users not bothering to use a VPN.
- Like all prior 3GPP technologies, 5G requires mutual authentication. Devices must authenticate with the network through sophisticated authentication keys. The ability to deny access to non-approved devices at the point of an initial authentication attempt is built in to 5G. In the U.S, licensed wireless operators require that a device must be certified for use. Uncertified devices that may interfere with the spectrum and the experience of other users are denied access.

For 5G, 3GPP has further extended encryption into parts of the security architecture where traffic was previously allowed to be in plaintext.

Encrypting against IMSI catchers and signaling interception

3GPP has a proven track record of delivering a strong cybersecurity roadmap for licensed wireless operators spanning different generations of the standards. For example for 5G it has further extended encryption into parts of the security architecture where traffic was previously allowed to be in plaintext.

- With 4G, so-called 'false base stations' or 'IMSI catchers' can potentially be used to capture unencrypted International Mobile Subscriber Identity (IMSI) numbers over the air and determine whether a target individual's phone is in the immediate area. In 5G, the equivalent of the IMSI is encrypted to prevent that.
- As captured by a notorious 2016 '60 Minutes' documentary showing how members of Congress could be all-too-easily spied on, a weakness in 4G standards enabled this by leaving SS7 and Diameter signaling traffic between mobile roaming partners unencrypted. The 5G security standards now encrypt this traffic to prevent that.

As well as embedding fixes for the above vulnerabilities in 5G security standards, 3GPP has also worked with wireless operators, vendors and other ecosystem partners to develop retrospective fixes for the same problem in older generations of the standards. For example, signaling firewalls are widely available for blocking malicious signaling messages in 2G, 3G and 4G roaming traffic. Solutions are also available that detect false base stations or IMSI catchers trying to exploit weaknesses in older 3GPP standards.

Spectrum Sharing Models Introduce New Cyber Threat Vectors

In cybersecurity, complexity always helps attackers and always hinders defenders. The licensed spectrum model offers clear cyber security advantages over complex database-driven shared spectrum mechanisms like the one Citizens Broadband Radio Service (CBRS) uses.

To give just one example, the CBRS model's dependence on a handful of centralized Spectrum Access System (SAS) databases to coordinate sharing introduces potential DDoS attack vectors. Compromised CBRS devices could potentially flood an SAS with communication, hence potentially preventing it from allocating spectrum to users.

Network and security operations to curate the wireless network

Best practise cybersecurity determines that the second 'protection' pillar of the NIST cybersecurity framework is necessary but not sufficient. In line with so-called Zero Trust principles, the working assumption has to be that a subset of cyber threats will inevitably penetrate whatever protections are put in place – hence no user, device, application or network can be inherently trusted. This is what drives the importance of best-in-class security operations. This monitors for known and unknown threats in the wireless network with strong detection and response as prescribed by the third and fourth pillars. Licensed wireless operators invest a lot in this kind of network and network security monitoring. Some even tie their operations teams' bonuses to specific Key Performance Indicators (KPIs) like dropped calls.

Jamming or blocking of wireless signals in licensed or unlicensed spectrum is illegal under the 1934 Communications Act. In practice, however, the licensed spectrum ecosystem is much better at defending against jamming.

Protecting wireless networks against jamming

Two different examples demonstrate the unique capabilities that licensed operators bring to bear in terms of assuring the availability of the wireless network. The first is jamming. From a legal perspective, jamming or blocking of wireless signals in licensed or unlicensed spectrum is illegal under the 1934 Communications Act. From a technical perspective, jamming is also just as easy to carry out in licensed or unlicensed spectrum.

In practice, however, the licensed spectrum ecosystem is much better at defending against jamming. With unlicensed spectrum, any jamming signal is typically dismissed by users as co-channel interference from other users. The user accepts the degradation in service, typically without even being aware that jamming is occurring. The licensed spectrum model is better at defending spectrum against jamming because wireless operators are permanently monitoring it. A sudden change in experience due to a jammer gets flagged up to the operations team as a performance degradation, allowing the operations team to investigate. Ultimately, a licensed wireless operator can work with law enforcement to identify, apprehend and prosecute an offender. There's no reason an unlicensed spectrum user can't do some or all of these things. It's just that in practice, it tends to be the exception rather than the rule whereas it's the rule in the case of the licensed spectrum ecosystem.

Certainly, jamming has presented a low risk to wireless networks up until now. The coverage zone or number of users that can be impacted is pretty small. Moreover, such motivations have been at least partially deterred by the risk of discovery and prosecution. Two factors have potential to increase risk here, though:

- The first is rising geopolitical tensions.
- The second is much better coordination of jamming devices or the development of better jamming devices.

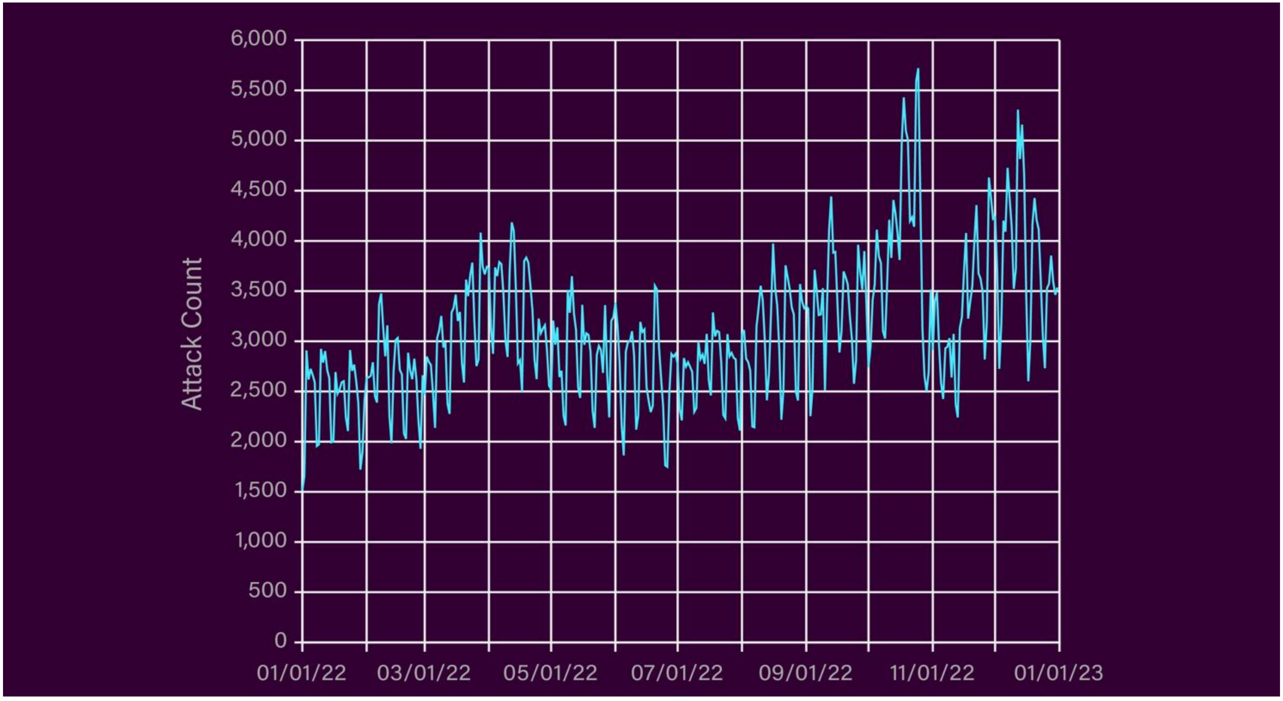
These factors could potentially combine to foster attacks that block communications across larger coverage areas, requiring a rapid, coordinated response by wireless operators and law enforcement.

A high level of investment in DDoS protection

A second example is what licensed operators do 24/7 to defend users against DDoS attacks. NETSCOUT Systems' 2H 2022 Threat Report shows that licensed operators drop 80% – 100% of high bandwidth attack traffic. They also mitigate 25% of attacks under 100 Mbit/s. That said, operators only recoup a subset of this cost from customers paying for protection against DDoS attacks that target them directly.

The operators shoulder a large portion of the total cost themselves to maintain service availability for all their customers - once again, it's in their interest. Most customers are not even aware of this; they just take it for granted. But this high level of investment is critical to minimizing network and service outages and degradations. If licensed operators only mitigated those DDoS attacks that their customers directly pay them to mitigate, world-wide media headlines would be pointing at the impacts within hours.

Figure 5: A Sharp Uptick in DDoS Attacks on Wireless Networks Throughout the World



Source: NETSCOUT 2H 2022, Threat Intelligence Report

The last year has seen a particularly marked uptick in the number of DDoS attacks on wireless networks that NETSCOUT has observed. As shown in **Figure 5**, NETSCOUT reports seeing peaks of more than 5,000 DDoS attacks per day on wireless networks from the end of 2022, up from 2,000 – 3,000 per day a few months earlier.

The effectiveness of any licensed wireless operator's cybersecurity operations is derived in part from its participation in a much broader cybersecurity ecosystem.

As mentioned, 5G FWA provides a contiguous security architecture between home and outdoor domains. An additional risk that has to be managed with FWA, however is that it exposes the wireless network to the exact same risk of DDoS and other attacks from poorly secured IoT devices in the home that cable and other fixed line ISPs have exposed their networks to for years. At least with licensed wireless operators, though, best practise network and security operations are in place and experienced at mitigating this sort of risk.

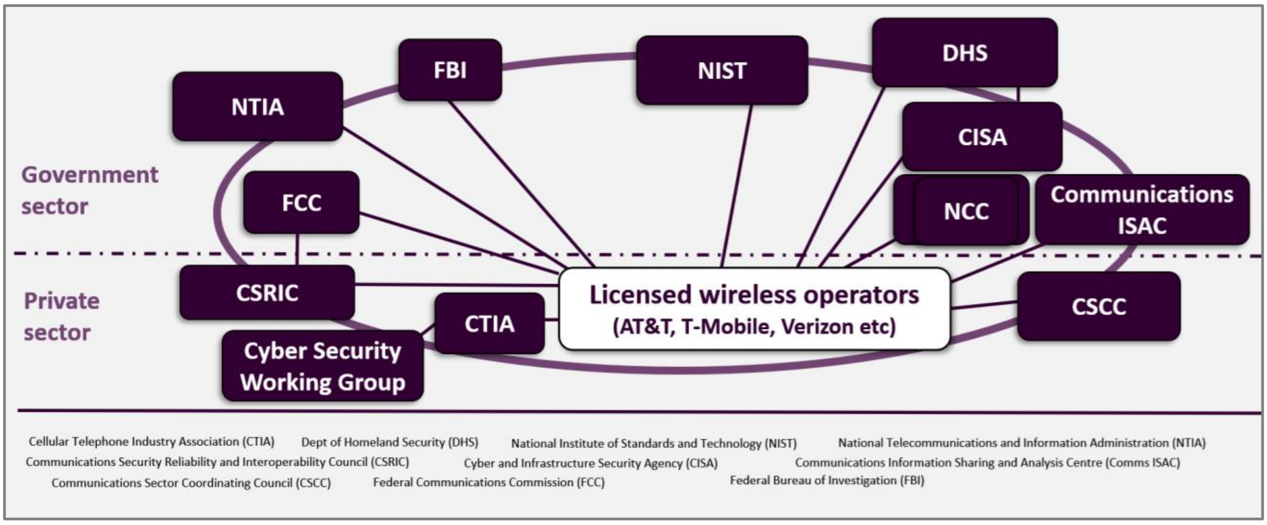
Proven cybersecurity collaboration with government and peers

In the U.S. the effectiveness of any licensed wireless operator's cybersecurity operations is derived in part from its participation in a much broader cybersecurity ecosystem as depicted in **Figure 6**. This protects the telecom sector itself but also leverages the telecom sector to protect other IT infrastructure, including critical infrastructure.

Some relationships in this ecosystem are hierarchical or top-down. For example, when the FBI obtains the authority for lawful interception, licensed wireless operators have to comply. They have an opportunity to try and shape the final outcome of FCC Notices of Proposed Rule Making, such as recent ones on emergency wireless alerts and mandatory incident reporting - but when the rules are finalized, they also have to comply.

Many of the other relationships depicted, however, are peer to peer or voluntary. For example, licensed wireless operators are key players in the FCC's Communications Security, Reliability, and Interoperability Council (CSRIC), augmenting wireless network security beyond 3GPP standards. They also collaborate in groups such as CTIA's Cyber Security Working Group (CSWG), whose 5G Security Test Bed launched in January 2022. Launched by founding members AT&T, Ericsson, T-Mobile, UScellular, MITRE, and the University of Maryland, the test bed primarily focuses on verifying the FCC's CSRIC VII recommendations for 5G networks.

Figure 6: Close Security Collaboration Between Government and Licensed Wireless Operators


Government sector
Private sector
NTIA
FBI
NIST
DHS
CISA
FCC
NCC
Communications ISAC
CSRIC
CTIA
Cyber Security Working Group
Licensed wireless operators (AT&T, T-Mobile, Verizon etc)
CSCC
Cellular Telephone Industry Association (CTIA)
Dept of Homeland Security (DHS)
National Institute of Standards and Technology (NIST)
National Telecommunications and Information Administration (NTIA)
Communications Security Reliability and Interoperability Council (CSRIC)
Cyber and Infrastructure Security Agency (CISA)
Communications Information Sharing and Analysis Centre (Comms ISAC)
Communications Sector Coordinating Council (CSCC)
Federal Communications Commission (FCC)
Federal Bureau of Investigation (FBI)

Source: HardenStance

Led by Director Jen Easterly, CISA is seeking to improve cyber threat intelligence sharing among stakeholders across the government and private sectors. This is widely considered to be in need of significant improvement. Among the various industry Information Sharing and Analysis Centres (ISACs) that come under CISA, however, the Communications Information Sharing and Analysis Centre (Communications ISAC), is well established and widely considered to be among the most effective. As well as in formal industry fora, wireless industry collaboration in cybersecurity also happens informally on the basis of personal, trusted, networks of peers in the U.S and abroad.

Unlike telecom operators using licensed spectrum, disaggregated networks using unlicensed or shared spectrum are not expected to be in a position to participate in data breach notifications.

In January 2023, the FCC brought forward a new Notice of Proposed Rule Making proposing to update the terms on which telecom operators must report cybersecurity incidents to the authorities. Unlike telecom operators using licensed spectrum, disaggregated networks using unlicensed or shared spectrum are not expected to be in a position to participate in data breach notifications.

The licensed wireless industry's response to a 911 hack

One example of what the wireless industry can achieve through collaboration in cybersecurity is its response to a notorious incident back in 2016. A teenage hacker, Meetkumar Hiteshbhai Desai, wrote code that caused iPhones to make repeated calls to Public Safety Answering Points (PSAPs). These are the dedicated call centres that respond to 911 calls.

Desai then published the code on social media, leading others to also use it as a "prank". The resulting Telephony Denial of Service (T-DoS) attacks on PSAPs in 12 states risked disruption to 911 services, putting lives at risk. The wireless industry's response to this incident resulted in a fix for the problem being developed and rolled out by all the major wireless carriers within 24 hours. This type of extensive, systematic, collaboration to achieve common goals, some of which may have major national security implications, is unique to wireless operators that use licensed spectrum.

Consistent security practices across licensed spectrum users

Wireless operators using licensed spectrum are driven to abide by norms in cybersecurity architecture and operations that extend well beyond a common baseline of advanced security baked into all 3GPP compliant hardware and software. The common commercial incentives, the common approach to security operations, the regulatory mandates and peer-to-peer collaboration, mean licensed wireless operators have a lot more in common than differentiates them from a cybersecurity perspective.

This alignment around common practices and shared objectives between private and government sectors is enormously important – from a national security perspective as well as from a broader cybersecurity perspective. Stakeholders are familiar with ways of responding to known cybersecurity incidents and are able to adapt those best practices to new events as and when they arise.

In this regard, the contrast with the world of unlicensed spectrum couldn't be more stark. Unlicensed spectrum users may use broadly similar technology building blocks and technical architectures. However, the variations in architecture and security operating model are inevitably a lot greater from one deployment to the next. Neither the FCC nor any other government agency has anything like the same expectations of unlicensed spectrum holders with respect to collaboration and accountability in areas like cyber incident reporting in the broader national interest.

About CTIA

CTIA represents the U.S. wireless communications industry. From carriers and equipment manufacturers to mobile app developers and content creators, we bring together a dynamic group of companies that enable consumers to lead a 21st Century connected life. www.ctia.org

About HardenStance

HardenStance provides trusted research, analysis and insight in IT and telecom security. HardenStance is a well-known voice in telecom and enterprise security, a leader in custom cybersecurity research, and a leading publisher of cybersecurity reports and White Papers. HardenStance is also a strong advocate of industry collaboration in cybersecurity. HardenStance openly supports the work of key industry associations, organizations and SDOs including NetSecOPEN, AMTSO, OASIS, The Cyber Threat Alliance, MEF, The GSMA, CTIA and ETSI. To learn more visit www.hardenstance.com

HardenStance Disclaimer

HardenStance Ltd has used its best efforts in collecting and preparing this report. HardenStance Ltd does not warrant the accuracy, completeness, currentness, noninfringement, merchantability or fitness for a particular purpose of any material covered by this report.

HardenStance Ltd shall not be liable for losses or injury caused in whole or part by HardenStance Ltd's negligence or by contingencies beyond HardenStance Ltd's control in compiling, preparing or disseminating this report, or for any decision made or action taken by user of this report in reliance on such information, or for any consequential, special, indirect or similar damages (including lost profits), even if HardenStance Ltd was advised of the possibility of the same.

The user of this report agrees that there is zero liability of HardenStance Ltd and its employees arising out of any kind of legal claim (whether in contract, tort or otherwise) arising in relation to the contents of this report.